

# GUIDANCE FOR COMPLETING A RISK ASSESSMENT

## **Purpose**

Management conducts a risk assessment in order to appropriately identify, measure, and prioritize risks so that the primary focus is placed on the areas of greatest significance. It also ensures that proper internal controls are in place to manage identified risks. The process can assist management in identifying problems or weaknesses and, with proper follow-through, results in improvements. The assessment reflects the perception, understanding and opinion of the evaluator (ideally someone with a solid working knowledge of the program/activity) and, when performed objectively, is a very good indicator of risk. Keep in mind that the existence of risk is not detrimental as long as it is recognized and properly controlled.

## **Approach**

- Managers' knowledge of the program's operations,
- The rationale for changes occurring in a program, function, or procedure; and
- The results of recent reviews or evaluations by the Office of the Inspector General, Government Accountability Office, or management evaluations.

**Risk Identification.** A risk is anything that could jeopardize the achievement of a goal. For each goal, risks should be identified. To help identify risks ask the following questions

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?
- How could someone steal from the Agency?
- How could someone disrupt our operations?
- How do we know whether we are achieving our goals?
- On what information do we most rely?
- On what do we spend the most money?
- How do we bill and collect our revenue?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- What is our greatest exposure?

## **Methods of risk identification**

- Qualitative approach - Identify and rank high-risk program/activity by defining risk in a subjective and general term such as high (possibility exists for misuse), medium (falls outside the parameters indicated for high and low), and low (small possibility) with reliance on expertise, experience and judgment (examples):

## GUIDANCE FOR COMPLETING A RISK ASSESSMENT

- establish criteria
- likelihood and frequency of occurrence
- Quantitative approach - Estimate the monetary cost of risk reduction based on (a) the likelihood that a damaging event will occur, (b) cost of potential loss and (c) costs of mitigating actions that would need to be taken if the anticipated risk occurs.

### Internal factors for risk identification (examples):

- down sizing
- changes in management responsibilities

### External factors for risk identification (examples):

- changing needs or expectations of the Congress, agency, and the public
- new legislation or regulations

### Inherent factors for risk identification (examples):

- size of budget, special concerns
- special concerns

It is important that risk identification be comprehensive at both the Agency level and at the program or activity level for operations, financial reporting, and compliance. Management should consider external and internal risk factors.

### **Risk Analysis:**

- Assess the likelihood (or frequency) of the risk occurring,
- Estimate the potential impact if the risk were to occur; consider both quantitative and qualitative costs; and
- Determine how the risk should be managed; decide what actions are necessary.